DIGITAL EVIDENCE COLLECTION FRAMEWORK FOR INTERNET OF THINGS

N.Kala[1]
Centre for Cyber Forensics and Information Security
University of Madras, Chennai, Tamil Nadu, India
E-mail ID:kalabaskar@gmail.com
M.P.Varun[2]
Student, MSc, Cyber Forensics and Information Security,
Centre for Cyber Forensics and Information Security
University of Madras, Chennai, Tamil Nadu, India
E-mail ID:varun4mp@gmail.com

Abstract- Today is the era of Internet of Things (IoT) where overwhelming entities with embedded computing functionalities with interoperability and communication ability are interlinked to provide a convenient service to the owner. It makes human life more convenient and dynamic. As with every industrial revolution emerges a new type of crime and associated challenges, IoT also raises issues on security and creates opportunities for cybercriminals to attack these areas, resulting in a direct impact on users. Several challenges are posed before the forensic investigator due to the complexity of IoT technology. Hence there is a dire need for digital forensic framework in IoT to tackle these challenges. This paper focuses on a methodology of collecting evidence from IoT devices and concerned networks.

Keywords: IoT, Digital Forensics, Evidence Collection.

INTRODUCTION

In the past several years technology became an inevitable part of human life. The dependency on cyberspace (the Internet) has been increasingly growing and pervading every of life. This means there is higher demand and usage of electronic devices. Life transformed when these devices became capable of inter-operating and communicating through internet which facilitated and speeded up daily activities. This led the scientific community to further develop electronic devices to cope with activity transformation. The last two decades represents an instance of the aforementioned facts where all these technological breakthroughs such as smartphones, sensors and tablets came in an assorted manner to formulate the Internet of Things concept. The positive impact of this advancement is evident in almost every discipline of human life and one cannot imagine abandoning or working without digital devices for asingle day. However, there is a dark side of using digital technology which comes in form of security breaches and vulnerabilities. These breaches may vary in types and ramifications and are extremely serious and may cause a massive loss if not addressed. The advent of IoT increased the concern as it creates opportunities for cybercriminals to attack these areas, resulting in a direct impact on users. Several numbers of challenges are posed before the forensic investigator investigating an IoT crime due to the complexity of IoT technology. Hence there is a dire need for digital forensic framework in IoT to tackle these challenges.

PROBLEM STATEMENT

A complex technology such as Internet of things poses several challenges in front of forensic investigator in collecting the evidences from an Internet of Things environment. It is hard to find where the IoT data exists, from where it comes from and how to scope down to potential evidence.

1. OBJECTIVES OF THE STUDY

i. To identify the IoT devices that is available.
ii. To identify the technology behind implementation of IoT devices.
iii. To study the emerging cybercrimes that is occurring in IoT environment.
iv. To study the issues and challenges in collecting the evidence from IoT devices for digital forensics investigation.
v. To identify the existing methods of collection of evidence from IoT devices.
vi. To propose a framework for digital forensics in the IoT environment.

2. RESEARCH QUESTIONS

Based on the above objectives following research questions were raised: -

1. What all are the IoT devices that are available in market?
2. What kind of technology is being implemented in IoT environment?
3. What are the emerging crimes targeting IoT environment?
4. What issues and challenges are faced by forensic investigators while collecting the evidence from IoT devices?
5. What are the existing methods for collection of evidence from IoT devices?
6. How to cope up with these challenges by framing a Digital Forensics framework customized for IoT environment?

3. INTERNET OF THINGS

The Internet of Things is a novel paradigm shift in Information Technology arena. The phrase "Internet of Things" which is alsowell-known as IoT is coined from the two words "Internet" and "Things". The Internet is a global system of interconnected computer networks that use the standard Internetprotocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millionsof private, public, academic, business, and government networks, of local to global scope, that are linked by abroad array of electronic, wireless and optical networking technologies. While the Things can be any object or person which can be distinguishable by the real world. Objects include not only electronic devices we encounter and use daily and technologically advanced products such as equipment and gadgets, but "things" that we do normally think of as electronic at all such as furniture, equipment's, materials etc. Things can be both living things like person, animals, plants or Non-living things such as home appliances or industry apparatus. So at this point, things are real objects in this physical or material world.

IoT can be defined as an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment. It is maturing and continues to be the latest, most hyped concept in the Information Technology world. Over the last decade the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and anyone. The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object.

IoT describes a world where just about anything can be connected and communicates in an intelligent fashion than ever before. Most of us think about "being connected" in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. But in the Internet of Things, sensors and actuators embedded in physical objects from roadways to pacemakers are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What's revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention. The "Internet of Things" refers to the coding and networking of everyday objects and things to render them individually machine-readable and traceable on the Internet.

4. IoT key features

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and use of small devices. A brief review of these features is given below:

Artificial Intelligence: IoT essentially makes virtually anything "smart" meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing refrigerator and cabinets to detect when milk and favourite cereal run low, and to then place an order with preferred grocer.

Connectivity: New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

Sensors: IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

Active Engagement: Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

Small Devices: Devices have become smaller, cheaper, and more powerful over time. IoT exploits purpose built small devices to deliver its precision, scalability, and versatility.

A. Harnessing the advantages from IoT

The advantages of IoT span across every area of lifestyle and business. Some of the advantages that IoT has to offer are: -

Improved Customer Engagement: Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.

Technology Optimization: The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

Reduced Waste: IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.

Enhanced Data Collection: Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyse our world. It allows an accurate picture of everything.

B. Significant set of challenges in IoT

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Some of the major issues are: -

Security: IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.

Privacy: The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.

Complexity: IoT systems are complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.

Flexibility: Flexibility of an IoT system to integrate easily with another is a concern.

Compliance: IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

C. The four-stage architecture of an IoT system:

Stage 1 of IoT architecture consists of networked things, typically wireless sensors and actuators. Stage 2 includes sensor data aggregation systems and analog-to-digital data conversion. In Stage 3, edge IT systems perform pre-processing of the data before it moves on to the data center or cloud. Finally, in Stage 4, the data is analyzed, managed, and stored on traditional back end data center systems. Clearly, the sensor/actuator state is the province of operations technology (OT) professionals. So is Stage 2. Stages 3 and 4 are typically controlled by IT, although the location of edge IT processing may be at a remote site or nearer to the data center.

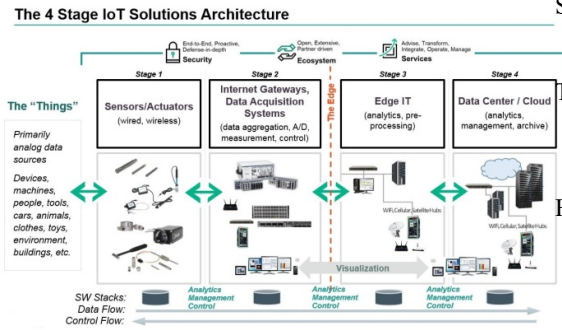

Figure 1: Stages for IoT architecture

D. IoT Sensors, Wearables and devices

The hardware utilized in IoT systems includes devices for a remote dashboard, devices for control, servers, a routing or bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications, security, communication, and detection to support-specific goals and actions.

E. IoT Sensors

The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, RF modules, and sensing modules. RF modules manage communications through their signal processing, Wi-Fi, ZigBee, Bluetooth, radio transceiver duplexer, and BAW. The sensing module manages sensing through assorted active and passive measurement devices. Given below is a list of some of the measurement devices used in IoT.

Table 1: Various types of sensors

Sensing Devices	
Accelerometers	Temperature Sensors
Magnetometers	Proximity Sensors
Gyroscopes	Image Sensors
Acoustic Sensors	Light Sensors
Pressure Sensors	Gas RFID Sensors
Humidity Sensors	Micro Flow Sensors

F. Smart wearable devices

Head :Helmets,glasses
Neck :Jewellery,collars
Arm :Watches,wristbands,rings
Torso :Clothing,backpacks
Feet : Socks, shoes

IoT Devices

Smart cities:
- Sensors monitoring vibration of building, bridges etc.
- Sensors monitoring trash condition

Transportation:
- Sensors for monitoring parking space
- Sensors for monitoring traffic conditions
- Smart car

Home automation:
- Smart TV
- Smart refrigerator
- Smart oven
- Smart meter for monitoring energy usage

EHealth:
- Smart caregiver wearables heart monitor
- Pain relief wearable Smart chair
- Smart scale

Smart environment:
- Sensor for monitoring forest fire
- Sensor for monitoring air condition
- Sensor for monitoring earthquake zone

Smart water:

Sensor for monitoring rivers for chemical leakage
Sensor for monitoring pipes for water leakage
Sensor for monitoring river for flood

Retail:

Sensor, RFID for storage conditions
Sensor, RFID for controlling rotation of products
Industrial control:
Sensor for controlling temperature during manufacturing

Smart agriculture:

Sensor for controlling amount of sugar in grapes
Sensor for controlling conditions in greenhouses
Sensor for tracking locations of animals

After reviewing the above literatures and studying the IoT technology, it was learned that there are lot of issue and challenges in IoT forensics so there is a dire need in proposing a framework for evidence collection in IoT environment. So the next chapter deals with IoT evidence collection framework.

5. IoT EVIDENCE COLLECTION FRAMEWORK

The Internet of Things (IoT) has facilitated the creation of numerous inter-connected smart gadgets like toasters, refrigerators, thermostats, locks, washing machines, car, garage doors, motion detectors etc. that connect to online services and platform. These devices being always connected produces new types of cyber physical evidentiary data. The acquisition of forensically relevant data and its analysis pose a challenge as the devices don't have a common interface, internal storage or standard protocol. Nevertheless, this shift towards inter-connected devices also bring new avenues for digital evidence like pinpointing the exact date and time a door was opened or locked, the temperature change, or when a car was parked, which in turn could help find digital evidence of forensic value in a potential case. In this project an IoT evidence collection framework is proposed to facilitate forensic collection evidences from multiple IoT devices.

A. Overview of the framework

This framework for IoT evidence collection undertakes two approaches that is preparing the IoT environment for Pre-Investigative readiness and preparing the IoT environment for real time smart forensics. In Pre-Investigative readiness preparation three approaches are suggested.

Zone-based method for approaching IoT related investigations

Establishing a central evidence collection point

Integrating the IoT environment details into the Building Information Model

In preparation of IoT environment for real time forensics an automated forensics system is suggested which provides Forensics as a Service (FaaS) to a certain degree until it is necessary to involve external experts. This framework integrates all these approaches and feeds the data from one system to another in an effort to scope down the collection of potential evidence in aIoT environment.

B. Framework Core

IoT evidence collection framework which is proposed to facilitate effective forensic collection of evidences from IoT environment consisting of multiple IoT devices revolves around two approaches that forms the core of the entire evidence collection process. They are:

- Preparing the IoT environment for Pre-Investigative readiness
- Preparing the IoT environment for real time smart forensics

C. Preparing the IoT environment for Pre-Investigative readiness

The Pre-investigative readiness is very essential step in ensuring the preparedness before any incident and also to enable the effective investigation. It involves preparation of entire infrastructure in such a manner as to ease the efforts of identifying and collecting the evidence for forensic investigation. Thus in actual sense it's a process of scoping down the essentialities which will help investigator to collect evidence in a faster and efficient manner. This research suggests and focuses on three key concepts that needs to be essentially be set up in an earlier stage prior to incident in order to achieve Pre-Investigative readiness.

These concepts are: -

1. Zone-based method for approaching IoT related investigations
2. Establishing a central evidence collection point
3. Integrating the IoT environment details into the Building Information Model

Though several researches have been done on these key concepts earlier, this approaches where visualized individually. This project presents a unified approach that combines all these key concepts and interlinks them to demonstrate the flow of information from one concept to another thus helping in scoping down the potential evidence for investigative purpose. The information from this phase will cater as input for a smart real time forensics in the later stage.

Pre-Investigative readiness addresses the following questions: -

- What the investigator as to identify?
- How the investigator will identify the potential evidence/devices?
- What the investigator as to collect?
- Where the investigator will find potential evidence/device?
- How the investigator will collect the potential evidence/devices?

D. Zone-based method for approaching IoT related investigations

Digital Forensics in IoT will involve knowing where the investigator has to look for evidence. Without any formal way for evidence collection valuable time will be wasted looking in the wrong places for irrelevant evidence. This framework proposes a zone based method for approaching IoT related investigations.

Zone 1: This is the internal zone where all hardware, software and networks (e.g. Bluetooth and Wi-Fi) exits. This zone comprises of devices such as mobile devices, smart wearable gadgets, gaming consoles, smart fridge, thermostat & heat controllers, locks, doors, camera, motion detectors, smart lightings, RFID tags, embedded systems and other house retrofits. In this zone the devices that relates to a crime scene is catalogued and a decision is made about what is relevant to the case and what may hold evidence that will be useful to the case. These devices are identified using tag identifications (tag ID) and their state i.e. asleep, awake, active/transmitting, ON, OFF etc.

FIGURE 2: IOT EVIDENCE COLLECTION FRAMEWORK

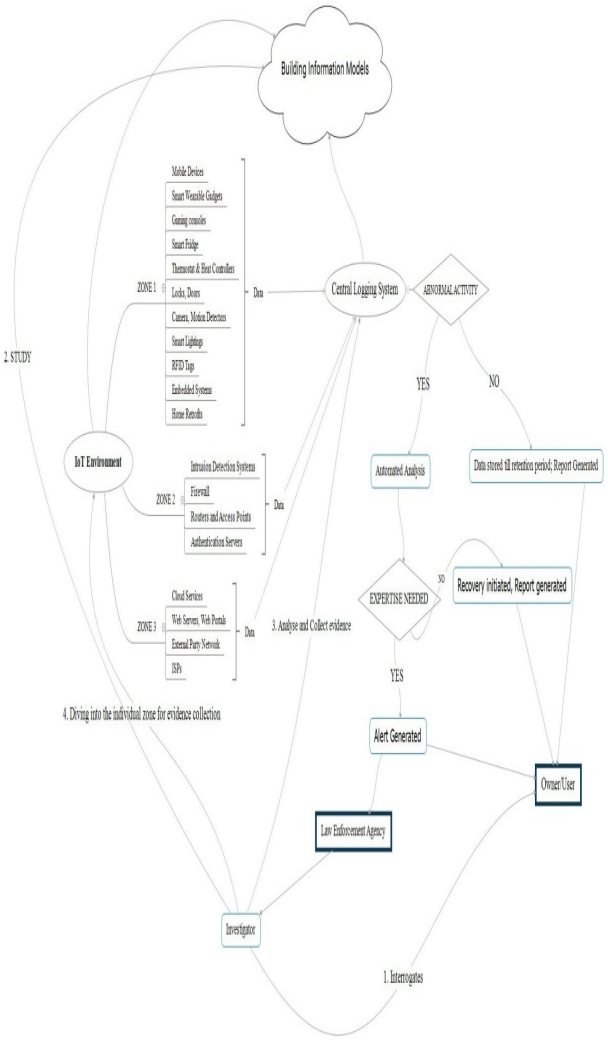

FIGURE 3: ZONES (1-2-3)- DIGITAL FORENSICS

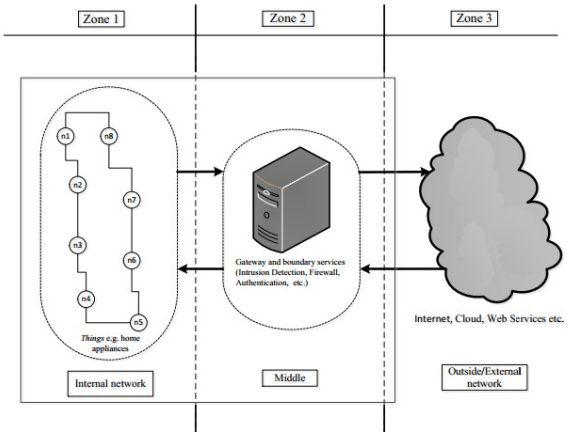

TABLE 2:
ZONE 1 DETAILS

Zone	Zone 1 (Internal devices)	
Devices	Mobile devices, Smart wearable gadgets, Gaming consoles, Smart fridge, Thermostat & heat controllers, Locks, Doors, Camera, Motion detectors, Smart lightings, RFID tags, Embedded systems, House retrofits.	
Attacks	Denial of service, Tampering of output, Distribution of malicious content, Data theft etc.	
Evidence	Sensor data (IP address, sensor ID)	State change data, Logs, etc.

Zone 2: All devices and software that are at the edge of the network and that provide a communication medium between the internal and external networks comes in Zone 2. This zone consists of all public-facing devices of the networks in question such as Intrusion Detection System, Intrusion Prevention System, Network Firewall, Routers, Access points

and Authentication systems. Forensics investigations will typically involve identifying these elements, cataloguing them and retrieving any available relevant evidence from them.

Table 3: Zone 2 Details

Zone	Zone 2 (Edge devices)
Devices	Intrusion Detection System, Intrusion Prevention System, Network Firewall, Routers, Access points, Authentication systems etc.
Attacks	Denial of service, Unauthorized intrusions, Data modifications etc.
Evidence	Network logs, intrusion traces etc.

Zone 3: This zone covers all hardware and software that is outside of the network. This zone includes evidence from all cloud, social network, Internet Service Provider (ISP), mobile network provider's data, internet and web based services and other external party networks (such as neighboursIoT network, hospital network etc.).

Table 4: Zone 3 Details

Zone	Zone 3 (External network)
Devices	Cloud, Social network, Internet Service Provider (ISP), Mobile network provider's data, Internet and web based services and other external party networks (such as neighbours IoT network, hospital network etc.).
Attacks	Privacy issues, Data theft, Impersonation, Fraud
Evidence	User activity data and logs

It is at the discretion of digital forensic investigator to apply this approach. Investigation can be done in parallel (all zones at same time) or zone of greatest priority can be identified based on the evidence gathered from the Central logging system. This approach reduces the complexity that will be encountered in IoT environments and ensures that investigators can focus on clearly identified areas and objects in preparation for investigations.

E. Establishing a Central Evidence Collection Point

This framework consists of a central evidence collection point known as Central logging system that collects data from the three different zones. Data such as state change (e.g. Door closed or opened) is a vital clue for the investigation. This evidence collection point collects data from the sensors, controllers and internal devices, edge network device such as firewall and user activities and state change logs form cloud. A controller can be used as a Central logging system. IoT controllers provide a centralized mechanism by which multiple IoT devices can connect to, be managed and controlled. Through a controller, developers and engineers can support a variety of hardware and communication platforms. These controllers can typically acquire and modify the state of an IoT device. A Central logging system should have the same functionality as an IoT controller but with forensics in mind.

Figure 4: Sensors data to central logging system

Sensors data to Central logging system: This is just like how a sensor gets connected to a controller. An example would be like an IP camera and an application residing on a computer within the same network used to control it. The camera registers a state change when it detects motion. This state change can be reported back to the central logging system where further actions can be taken based on the identified state change.

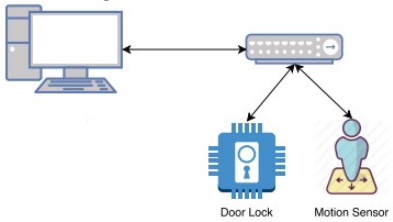

Figure 5: Controller data to central logging system

Controllers to Central logging system: Controllers connect to internet to allow control of connected devices through web interfaces. Thus it is proposed to input its data to the central logging system. By accessing the controller, the state change logs of multiple devices can be acquired. This is a lucrative data collection point. As the number IoT devices increase their will be a dire need for such a centralized control. It provides a consolidated state for collecting state data of multiple devices.

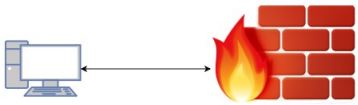

Figure 6: Edge Network Device data to Central Logging System

Edge devices to Central logging system: The Intrusion Prevention System, Intrusion Detection System, Network Firewalls sends their logs, details of malicious traffic detected, their state information to the central logging system. This information is vital for the system to analyse for abnormalities.

Figure 7: Cloud Data to Central Logging system

External network (Cloud) to Central logging system: Today IoT devices use cloud services as point of control and data collection. This provides a possibility of obtaining user activity details and change logs from cloud data by leveraging APIs which are used to manage IoT devices over internet. Thus by constructing individual scripts central logging system will receive its communication through calls to the cloud.

F. Characteristics of a Central logging system:

- Forensic soundness: A Central logging system can only acquire state data from IoT devices and is not allowed to change the state of an IoT device.
- Date & time logging: A Central logging system should be capable of accurately logging the dates and times of state changes.
- Secure storage and integrity: A Central logging system should embody secure storage of the collected IoT state data, and should also hash the collected states at the time of collection for later validation.
- Time Synchronization: As in the real-time approach for IoT forensic, the clock of the IoT devices, data storages, and detection mechanism must be timely synchronize. Therefore, these components must be able to meet the timing requirement, for instance, the deadline, period time and jitter. In the IoT context, the process usually ties with the deadlines and limited resources. And sometimes they need to run continuously for long periods of time without maintenance.
- Memory and Storage Requirement: Real-time computing requires having enough memory and storage capacity to accommodate the excessive processing and memory requirements and timing characteristics. In this approach, since the IoT devices have limitation in components, all the possible evidence is collected and stored in the central logging system.
- Communication Requirement: Strong and stable communication among component is vital to ensure that all the potential evidence can be extract and store in a timely manner.

G.Integrating the IoT and the Building Information Modelling

"Building Information Modelling (BIM) is a digital representation of physical and functional characteristics of a facility. A BIM is a shared knowledge resource for information about a facility forming a reliable basis for decisions during its life-cycle; defined as existing from earliest conception to demolition" (NBIMS-US, 2016). BIM is the process spanning the generation and management of the physical and functional information of a project. The output of the process is what we refer to as BIMs or building information models which are ultimately digital files that describe every aspect of the project and support decision-making throughout a project cycle. BIM and the subsets of BIM systems and similar technologies feature are more than just 3D (width, height, and depth) but may include further dimensions such as 4D (time), 5D (cost), and even 6D (as-built operation) (Smith, 2014).

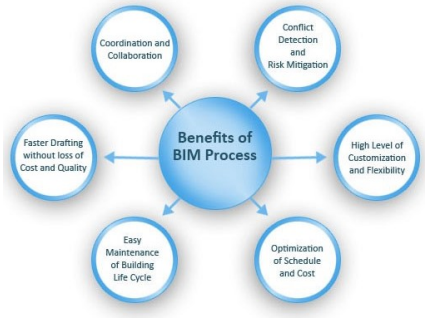

Figure 8: BIM Benefits

This framework suggests the integration of IoT environment details with the Building Information Modelling. By combining the information about the IoT capabilities of a building or structure, it may be possible to answer the questions of; where has the information come from? Where is the information stored? It is also crucial to identify in what format the data is stored or encoded. This would narrow the scope of the investigation, and enable the selection of features or data that identifies an individual user from a much smaller data set. A composite picture of the data gathered about an individual user could be constructed from the data stored or forwarded by the buildings they have inhabited.

Advantage to the investigation process:

BIMs presents the entire network architecture of IoT devices present in the building. The different technology used and their interconnection. It will also detail the various controls implemented for achieving the pre investigative preparedness. All the documentation reading IoT implementation will be integrated with details about device specifications, locations, vendor details.

BIMs will help the investigator to study the entirety of the environment (building), the various IoT network implemented, its corresponding details thus coping down to potential locations for evidence collection.

H. Preparing the IoT environment for real time smart forensics

This framework suggests a real-time approach for IoT forensics. Real-time in this context is referred as an automatic investigation on the IoT device. This approach is undertaken to accommodate the issue of handling the diversity of devices and to deal with various IoT constraints. The detection mechanism is deployed in this context will trigger the forensic phase if there are any abnormal activities detected on the IoT devices. Once detected the system start its process and takes necessary actions. The framework takes into cognizance the nature of the IoT and provides Forensics as a Service (FaaS) to a certain degree until it is necessary to involve external experts. The Real-time approach is essential as speed of response is crucial in IoT. User must be enabled to keep personal IoT under forensics surveillance by the use of adaptable and commercially forensics solutions.

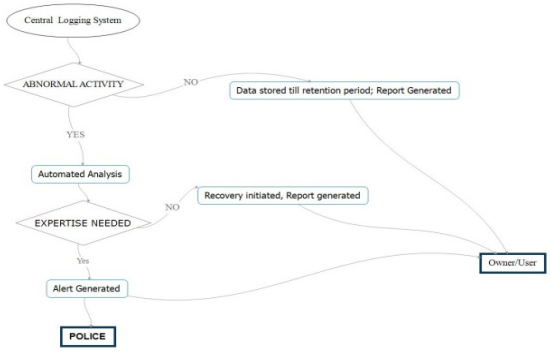

Figure 12: Real time smart forensics

The steps involved in real time smart forensics is clearly illustrated in Figure 12. This framework takes into cognisance the nature of the IoT and provides Forensics as a Service (FaaS) to a certain degree until it is necessary to involve external experts.

i. The central Logging System collects and monitors the data (State change, alert logs) form the different zones of IoT environment.

ii. Since large amount of data is transferred every moment, a continuous analysis is required to find abnormal activities. If no such activities detected, then the data is stored till retention period. If there is false alert, a report is generated and sent to user/owner.

iii. On identification of an abnormal activity, an automated analysis is carried out and the severity of the incident is determined.

iv. Based on the analysis, incident that doesn't require expertise is handled by the system itself by initiating recover. Report is generated and sent to user/owner.

v. If expertise is needed to handle that particular incident, then alert is generated and the law enforcement agency or other relevant agencies are informed. A report is also sent to user/owner.

Advantages of Preparing the IoT environment for real time smart forensics:

- Adaptable and easy to use/manage by end users themselves in the event of a security incident.
- Easy as changing light bulbs for home owners and as deploying their own forensics centres for large businesses.
- Can be integrated into a forensics system which can be deployed in homes and similar environments to carry out basic forensics (and security) functions including capturing and sifting through relevant data and producing evidence that is understandable and useful to home owners and law enforcement.

Framework Workflow

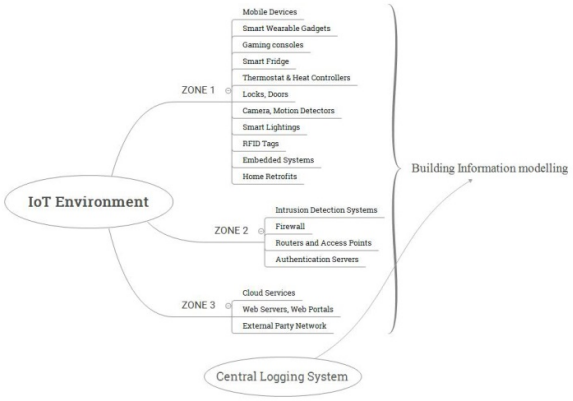

Figure 13: Classifying into Zones and integration with Building Information Modelling

The first phase proposed by this framework is classification of IoT environment into three zones. This will help investigator in knowing where to look for the evidence. Without any formal way for evidence collection valuable time will be wasted looking in the wrong places for irrelevant evidence.

IoT environment is divided into three zones:

Zone 1: This zone consists of internal devices such as mobile devices, smart wearable gadgets, gaming consoles, smart fridge, thermostat & heat controllers, locks, doors, camera, motion detectors, smart lightings, RFID tags, embedded systems, house retrofits.

Zone 2: This zone consists of network edge devices such as intrusion detection system, intrusion prevention system, network firewall, routers, access points, authentication systems etc.

Zone 3: This zone consists of external network such as cloud, social network, internet service provider (ISP), mobile network provider's data, internet and web based services and other external party networks (such as neighbours IoT network, hospital network etc.).

All these details are integrated into the Building Information Modeling. By combining the information about the IoT capabilities of a building or structure, it may be possible to

answer the questions of; where has the information come from? Where is the information stored? It is also crucial to identify in what format the data is stored or encoded. This would narrow the scope of the investigation, and enable the selection of features or data that identifies an individual user from a much smaller data set. By combining the information about a composite picture of the data gathered about an individual user could be constructed from the data stored or forwarded by the buildings they have inhabited. BIMs presents the entire network architecture of IoT devices present in the building. The different technology used and their interconnection. It will also detail the various controls implemented for achieving the pre investigative preparedness. All the documentation reading IoT implementation will be integrated with details about device specifications, locations, vendor details. It will help the investigator to study the entirety of the environment (building), the various IoT network implemented, its corresponding details thus scoping down to potential locations for evidence collection.

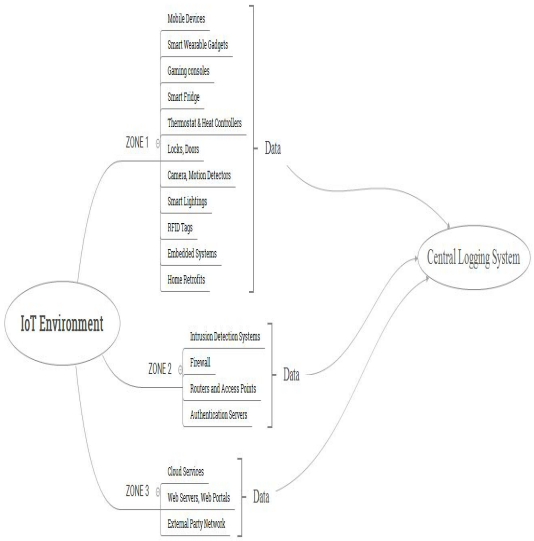

Figure 14: Feeding data into Central Logging System

In the next phase a Central Logging System is proposed which will record the data's (State change logs and alerts) from the different zones for analysis. E.g. When zone 1 devices register a state change it is reported back to the central logging system where further actions can be taken based on the identified state change. In same way data is fed from controllers and network edge devices like firewall. It shall also use cloud services as point of control and data collection. This provides a possibility of obtaining user activity details and change logs from cloud data by leveraging APIs which are used to manage IoT devices over internet.

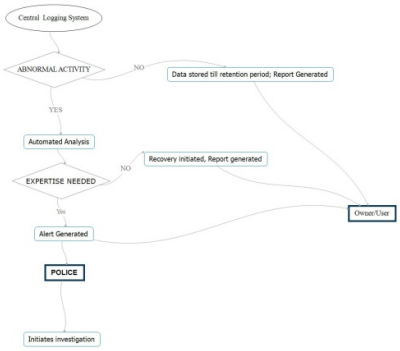

Figure 15: Initiating automated analysis and reporting

This framework takes into cognisance the nature of the IoT and provides Forensics as a Service (FaaS) to a certain degree until it is necessary to involve external experts. The central Logging System collects and monitors the data (State change, alert logs) form the different zones of IoT environment. Since large amount of data is transferred every moment, a continuous analysis is required to find abnormal activities. If no such activities detected, then the data is stored till retention period. If there is false alert, a report is generated and sent to user/owner. On identification of an abnormal activity, an automated analysis is carried out and the severity of the incident is determined. Based on the analysis, incident that doesn't require expertise is handled by the system itself by initiating recover. Report is generated and sent to user/owner. If expertise is needed to handle that particular incident, then alert is generated and the law enforcement agency or other relevant agencies are informed. A report is also sent to user/owner. This sets the investigation process.

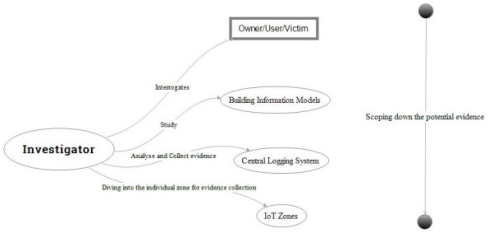

Figure 16: Initiating automated analysis and reporting

In the last phase investigator interrogates the relevant parties, then studies the BIMs for better understanding of the environment. This gives investigator insight into not only the IoT environment but also the entire physical, functional aspects of the environment such as building and also an insight into the life of person interacting with that environment. With this information in hand investigator analyse and collects evidence from the central logging system. Since the alert was initiated with a report from the same system, investigator can straight way scope down to objects of forensic interest. Investigator will then analyse the remaining data to gather potential relevant evidence. If a situation arises in need of great degree of information, investigator will

conduct investigation into the individual zones and collect evidence form IoT devices by image acquisition or memory forensics. At last evidences will be gathered, event will be reconstructed, examined and the investigator will present the report to court.

J. LIMITATION OF THIS FRAMEWORK

- The forensic framework proposed here has not been implemented, deployed and tested.
- It was assumed that implementation of the model will be scalable for growing number of devices.
- This framework is through the view point of a smart building only.
- The framework does not address the issue of connectivity to different IoT devices. There is a lack of standardization due to different wireless communication technologies, operating software and interfaces. So it is necessary to have hardware that supports these technologies.
- The challenge of examination of individual IoT devices is outside the ambit of the proposed framework.
- The framework does not address how exactly a malicious incident can be contained from spreading across the IoT network and the investigators decision regarding the state of devices (ON/OFF).

6. CONCLUSION

Is this era of Internet of Things (IoT) where overwhelming entities with embedded computing functionalities with interoperability and communication ability are interlinked to provide a convenient service to the owner. It makes human life more convenient and dynamic. As with every industrial revolution emerges a new type of crime and associated challenges, IoT also raises issues on security and creates opportunities for cybercriminals to attack these areas, resulting in a direct impact on users. Several number of challenges are posed before the forensic investigator due to the complexity of IoT technology. Hence there is a dire need for digital forensic framework in IoT to tackle these challenges. So this project focused on a methodology of collecting evidence from IoT devices and concerned networks.

In view of this, a study was done on various IoT devices available in market. It was learned that all these devices are basically combination of sensors, actuators embedded into devices with processing power. Learning the technology behind implementation of IoT framework was an objective. It was learned that Radio Frequency Identification (RFID), Wireless Fidelity (Wi-Fi), ZigBee, Near Filed Communication (NFC), Artificial Intelligence (AI), Sensor technology etc. forms the backbone of IoT network. IoT architecture models were discussed in detail and the concept is implemented in the framework.

Analysis was done on various emerging crime in IoT environment. It looked into the possibility of crime in various stages of IoT life cycle such as manufacturing, installation and operations. A reference is made to United Kingdom's government publication educating the citizen about various crime that can take place in individual's space and business environment utilizing IoT technology.

This research focused on various issues and challenges in collecting the evidence from IoT devices for digital forensics investigation. It was learned that enormous amount data flow poses a challenge to investigator in scoping down to potential evidence. The lack of standardization of IoT technology, lack of tools to interface with the IoT devices, issue of trans-border data flow are some of the challenges. Present day forensic framework developed by NIST and McKemmish were studied and it was identified that these existing framework could not cater well to the growing needs of IoT forensics which is again a driving force for the need to have a forensic framework customized for IoT environment.

Hence to address these challenges this project suggests an evidence collection framework for IoT environment. The proposed framework is based on two approaches that is preparing the IoT environment for Pre-Investigative readiness and preparing the IoT environment for real time based forensic method for approaching IoT related investigations. To achieve Pre-Investigative readiness, the framework suggests implementation of Zone-based method for approaching IoT related investigations where the IoT environment is divided into three zones based on the internal devices, edge network devices and external environment. This approach helps in scoping down the potential evidence for forensic investigator. Another suggestion is to establish a central evidence collection point which will collect state change logs and other alerts from these IoT devices and analyse the data for any possible abnormality. In case of any abnormality a smart forensic process is initiated to restore the issue or alert the relevant parties based on criticality of incident. This approach saves lot of time for forensic investigator and supports quick response initiation in IoT environment. Lastly the framework suggests the integration of IoT environment details with the Building Information modeling process. These BIMs serves as a vital information repository for the forensic investigator who is absolutely new to the IoT crime scene. By studying the BIMs, the investigator updates his/her knowledge about the facility, its functional, operational components, the life of the occupants and the various IoT devices that are established in that environment.

Lastly, the proposed framework aims at facilitating easy and less cumbersome method for collecting evidence in IoT environment and provides Forensics as a Service (FaaS) to a certain degree until it is necessary to involve external experts.

REFERENCES

1. Prof.S.A.Shaikh, Aparna S. Kapare, Associate Professor P.R.E.C, Loni, P.G Student, P.R.E.C, Loni, Smart Office Area Monitoring and Control Based on IoTInternational Journal of Engineering Research in Computer Science and Engineering(IJERCSE) Volume 4, Issue 4, April 2017.
2. RenukaBhuyar, Saniya Ansari, Design and Implementation of Smart Office Automation System, International Journal of Computer Applications (0975 – 8887), Volume 151 – No.3, October 2016.
3. Mohamed HishamMoubarak, Internet of Things for Home Automation, Media Engineering and Technology Faculty German University in Cairo
4. OnurSavas, Julia Deng, Big Data Analytics in Cybersecurity, Auerbach Publications; 1 edition (18 September 2017)
5. Mrs.Jyotsna P. Gabhane, Ms Shradha Thakare2, Ms.Monika Craig, Smart Homes System Using Internet-of-Things: Issues, Solutions and Recent Research Directions, International Research Journal of Engineering and Technology (IRJET)
6. Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei, Design of an Internet of Things-based smart home system, Intelligent Control and Information Processing (ICICIP), 2011 2nd International Conference on 25-28 July 2011
7. Intels Publication 1115/BB/CMD/PDF Fast, Secure, and Flexible Smart Office Solution
8. BhagyashriKatole, ManikantaSivapala, 3Suresh V, Principle Elements and Framework of Internet of Things, Research Inventy: International Journal of Engineering And Science Vol.3, Issue 5(July 2013)
9. Mr.AlgimantasVenčkauskas, Mr.Robertas Damasevicius, Mr. Vacuum Jusas, Mr.JevgenijusToldinas, A review of cyber-crime in internet of things: technologies, investigation methods and digital forensics, International journal of engineering sciences & research technology
10. UK government publication, Internet of Things Potential risk of crime and how to prevent it, Home Office and UCL (University College London)
11. Bill Montgomery, The 10 Most Terrifying IoT Security Breaches you aren't aware of (so far), https://www.linkedin.com/pulse/10-most-terrifying-iot-security-breaches-so-far-you-arent-montgomery
12. Nurul Huda NikZulkipli, Ahmed Alenezi and Gary B. Wills, IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things Conference,
13. R.C. Hegarty, D.J. Lamb and A. Attwood Digital Evidence Challenges in the Internet of Things, School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University, John Dalton Building, Chester Street, Manchester, UK School of Computing & Mathematical Sciences, 3School of Engineering, Technology and Maritime Operations, Liverpool John Moores University James Parsons Building, Byrom Street, Liverpool, UK
14. Parag H. Rughani, IoT Evidence Acquisition – Issues and Challenges, Gujarat Forensic Sciences University
15. SaadAlabdulsalam, Kevin Schaefer, TaharKechadi and Nhien-An LeKhac, Internet of things forensics: challenges and case study
16. Christopher S. Meffert, Christopher S. Meffert, Ibrahim Baggili, Ibrahim Baggili Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition
17. The National Institute of Standards and Technology (NIST), Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86
18. Rodney McKemmish, No. 118 What is Forensic Computing?
19. ISACA, Overview of Digital Forensics
20. Internet of Things, tutorials point, ://tutorialspoint.com/internet_of_things/index.htm
21. Internet of Things Principles and Paradigms, RajkumarBuyya, Amir VahidDastjerdi, Todd Green publication, ISBN: 978-0-12-805395-9
22. The 4 stages of an IoT architecture, https://techbeacon.com/4-stages-iot-architecture
23. SomayyaMadakam, R. Ramaswamy, SiddharthTripathi, Internet of Things (IoT): A Literature Review, Journal of Computer and Communications, 2015, 3, 164-173
24. EdewedeOriwoh, David Jazani, Gregory Epiphaniou, Paul Sant, Internet of Things Forensics: Challenges and Approaches
25. What is BIM? What are its Benefits to the Construction Industry?–APROPLAN https://www.aproplan.com/blog/quality-management-plan-construction/what-is-bim